The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
9/10/2009

SUBJECT:
Multiple Vulnerabilities in Apple QuickTime Player Could Allow for Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Apple QuickTime Player. Apple QuickTime Player is used to play media files on Microsoft Windows and Mac OS X operating systems. These vulnerabilities can be exploited if a user has a vulnerable version of Apple QuickTime Player and visits a malicious webpage or opens a malicious file, including an e-mail attachment. Successful exploitation will result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

- Apple QuickTime Player all versions prior to 7.6.4

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

DESCRIPTION:
Multiple vulnerabilities have been discovered in Apple QuickTime Player. These vulnerabilities are due to three types of flaws in the application.

The first flaw is a heap-based buffer-overflow issue due to the application failing to perform adequate boundary checks on user-supplied data. This problem occurs when handling FlashPix files or H.264 video files.

The second flaw in the application is a memory corruption issue due to the application failing to perform adequate boundary checks on user-supplied data. This problem occurs when handling malformed H.264 video files.

The third flaw in the application is in the way Apple QuickTime Player handles MPEG-4 video files. Opening a malicious video file can cause either an unexpected application termination or code execution on the victim's computer.

These vulnerabilities can be exploited if a user has a vulnerable version of Apple QuickTime Player and visits a malicious webpage or opens a malicious file, including an e-mail attachment. Successful exploitation will result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts may result in denial-of-service conditions.

RECOMMENDATIONS:

The following actions should be taken:

- Apply the appropriate update provided by Apple to vulnerable systems immediately after appropriate testing. The update is available at: http://www.apple.com/quicktime/download/
- Remind users not to download or open files from un-trusted websites.
- Remind users not to open email attachments from unknown or un-trusted sources.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

REFERENCES:

Apple:
http://support.apple.com/kb/HT3859
http://www.apple.com/quicktime/download/

Security Focus:
http://www.securityfocus.com/advisories/17856
http://www.securityfocus.com/bid/36328

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2202
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2203
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2798
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2799

Vupen Security:
http://www.vupen.com/english/advisories/2009/2584

Secunia:
http://secunia.com/advisories/36627/